(Under) Investment in cyber skills and data protection enforcement
Evidence from the UK Information Commissioner’s Office activity logs

Pantelis Koutroumpis   Farshad Ravashan   Taheya Tarannum

Oxford Martin School

August, 2023
In one internet minute ...

- 16M texts sent
- 5.9M Google searches
- 86K Instagram photos
- 347.2K Twitter tweets
- 2.43M Snapchat snaps
- 1.1M Tinder swipes
- 164.6K Zoom meeting hours
- 443K Amazon shoppers spend
- 437.6K Venmo users spend
- $98.2M in cryptocurrency spent
- 2.9M online event goers purchase
- 12.9K DoorDash diners place
- 76.4K in orders
- 1M streaming hours
In one evil internet minute ...

- 375 new cybersecurity threats will emerge.
- 16,172 records will be compromised.
- $1.63 million will be lost.
Motivation

An agency problem

- Cyber attacks often cause data breaches: Loss of personal data for customers but low direct costs for firms.
- Leads firms to underinvest in cyber security.

(Kankanhalli et al., 2003; Gordon et al., 2015a,b; Kopp et al., 2017; De Cornière and Taylor, 2021; Bana et al., 2021)
Motivation

An agency problem

- Cyber attacks often cause data breaches: Loss of personal data for customers but low direct costs for firms.
- Leads firms to underinvest in cyber security.
  \cite{kankanhalli2003, gordon2015a, gordon2015b, kopp2017, decorniere2021, bana2021}

An institutional factor

- Data protection regulation and laws are crucial for internalizing the social costs of cyber attacks into firms’ private costs.
Motivation

An agency problem

- Cyber attacks often cause data breaches: Loss of personal data for customers but low direct costs for firms.
- Leads firms to underinvest in cyber security.
  (Kankanhalli et al., 2003; Gordon et al., 2015a,b; Kopp et al., 2017; De Cornière and Taylor, 2021; Bana et al., 2021)

An institutional factor

- Data protection regulation and laws are crucial for internalizing the social costs of cyber attacks into firms’ private costs.

Research question

- Does stronger data protection alleviate the effects of these misaligned incentives? We address this question by examining the effect on firms’ cybersecurity hiring
Temporal variation

- We Study two legal changes in data protection regulations in the UK that enforced by Information Commissioners’ Office (ICO)
  
  - **Change in law enforcement**: Removal of requirement to prove ‘substantial damage or distress (SDD)’ in 2015.
  
  - **Change in law content**: Enactment of the DPA 2018 (UK-GDPR) that increased the ceiling of maximum monetary penalties.
This Paper

Temporal variation

- We Study two legal changes in data protection regulations in the UK that enforced by Information Commissioners’ Office (ICO)
  - **Change in law enforcement**: Removal of requirement to prove ‘substantial damage or distress (SDD)’ in 2015.
  - **Change in law content**: Enactment of the DPA 2018 (UK-GDPR) that increased the ceiling of maximum monetary penalties.

Sectoral variation

- **Novel data**: Exploit ICO activity logs and supervisory actions to build an index for exposure to data protection enforcement.
Our Findings

Quantitative effects: Data protection law is an effective device to incentivize firms to invest in cyber skills.

- 26% ↑ after the SDD removal.
- Up to 51% ↑ after the DPA 2018.

Qualitative effects: The response was stronger for
- Data-intensive firms
- Firms that invest in cloud
- Firms with ex-ante high cash holding

Economic trade-off: Slow down of firm dynamics; 12% ↓ in firm entry and 10% ↓ in firm exit.
Our Findings

**Quantitative effects:** Data protection law is an effective device to incentivize firms to invest in cyber skills.

- 26% ↑ after the SDD removal.
- Up to 51% ↑ after the DPA 2018.

**Qualitative effects:** The response was stronger for

- Data-intensive firms
- Firms that invest in cloud
- Firms with ex-ante high cash holding
Our Findings

**Quantitative effects:** Data protection law is an effective device to incentivize firms to invest in cyber skills.

- 26% ↑ after the SDD removal.
- Up to 51% ↑ after the DPA 2018.

**Qualitative effects:** The response was stronger for

- Data-intensive firms
- Firms that invest in cloud
- Firms with ex-ante high cash holding

**Economic trade-off:** Slow down of firm dynamics; 12% ↓ in firm entry and 10% ↓ in firm exit.
Overview

- Institutional set-up
  - UK Information Commissioner’s Office
  - Legal status and institutional changes

- Empirical strategy

- Results

- Concluding remarks
Institutional Set-up
How ICO processes the complaints

The ICO receives complaints

A case officer determines whether a breach has occurred

Yes

Determines what action is required

Strict: Monetary Penalties & Enforcement Notices

No

Case closed

Soft: Improvement Action Plans

Very Soft: One-Off Actions & Advice
ICO Timeline

Prior to 2010

- Limited Power (enforcement notices, undertakings, prosecutions, etc.)

2010

- Power to issue monetary penalties (up to £500,000)

2015

- Requirement to prove substantial damage and distress (SDD) is relaxed by PECR amendment

2016

- DPA 2018/EU GDPR is announced

2018

- DPA 2018 and GDPR come into effect (maximum fine up to £17.5 million or 4% of global annual turnover)
ICO enforcement trends

Removal of SDD clause → DPA 2018 announcement → DPA 2018 enactment (Mega fines introduced)

- Strict: Monetary penalties and enforcement notices
- Soft: Improvement action plans
- Very soft: One-off actions and advice

Date range: 2012 to 2019
What we do in 4 slides
Measuring sectoral exposure to ICO enforcement (1/4)

- Match with the UK business register to identify high vs. low exposure industries
Defining cyber skills from job postings data (2/4)
Using temporal variation of legal changes (3/4)

- Removal of SDD clause
- Passage of DPA 2018 (enacting GDPR in UK)

![Graph showing the share of cyber jobs in total job posting (%) over years 2012 to 2020, with markers for industries with high and low exposure to ICO actions.](image-url)
Empirical strategy (4/4)

**TTWA-Level Analysis**

\[
\text{cyber\_share}_{cjt} = \beta_1 \text{high ico exposure}_j \times SDD_t \\
+ \beta_2 \text{high ico exposure}_j \times DPA_t + \delta_{ct} + \rho_{cj} + \epsilon_{cjt}
\]

**Firm-Level Analysis**

\[
\text{cyber\_share}_{icjt} = \beta_1 \text{high ico exposure}_j \times SDD_t \\
+ \beta_2 \text{high ico exposure}_j \times DPA_t + \delta_{ct} + \mu_i + \epsilon_{icjt}
\]

- c: TTWA, j: 3-digit industry, t: year, i: firm.

- \(\epsilon_{icjt}\) and \(\epsilon_{icjt}\) double clustered at the 3-digit industry level and at the year level
Results
Result 1: Demand for cyber skills

(a) TTWA-level results

(b) Firm-level results

- SDD: Increased enforcement (2015-18): 26% ↑
- DPA 2018: Increased penalty (post-'18): 52% ↑

- SDD: Increased enforcement (2015-18): 37% ↑
- DPA 2018: Increased penalty (post-'18): 73% ↑
Result 2: Differential response by firm’s tech. portfolio

- Stronger response for firms investing in data harvesting skills (e.g. data mining, BI, ETL, AI, and big data).

- 6 times higher↑ among firms with cloud technologies after the passage of the DPA 2018.
Result 3: Differential response by firm’s cash holding

(a) Low cash holding

(b) High cash holding

<table>
<thead>
<tr>
<th>Dependent variable: % cyber job postings</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>High ICO exposure × Increased enforcement</td>
<td>0.053** (0.021)</td>
<td>0.065* (0.031)</td>
</tr>
<tr>
<td>High ICO exposure × Increased penalty</td>
<td>0.071* (0.034)</td>
<td>0.135** (0.042)</td>
</tr>
<tr>
<td>Firm FE</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TTWA × Year</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Observations</td>
<td>149780</td>
<td>124585</td>
</tr>
</tbody>
</table>
Result 4: Adverse effect on firm dynamics

(a) Birth rate

(b) Death rate

Post SDD
- Firm birth rate 0.6% ↓ (insig.), Firm death rate 0.9% ↑

Post DPA:
- Firm birth rate 1.4% ↓, Firm death rate 0.7% ↑
- Economic magnitude: 12% lower birth rate, 10% higher death rate.
Concluding remarks
Key points

- Impact of enforcement and content of laws: Regulatory tools are effective in correcting underinvestment in necessary cyber skills.
Key points

- Impact of enforcement and content of laws: Regulatory tools are effective in correcting underinvestment in necessary cyber skills.

- Trade-off between enhancing cybersecurity and firm dynamism.
Key points

- Impact of enforcement and content of laws: Regulatory tools are effective in correcting underinvestment in necessary cyber skills.

- Trade-off between enhancing cybersecurity and firm dynamism.

- The negative effects of GDPR: Data access vs. data security.
Thank you
## Baseline table

<table>
<thead>
<tr>
<th>SDD: High ICO exposure × Increased enforcement</th>
<th>TTWA level</th>
<th>Firm level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.264**</td>
<td>0.048**</td>
</tr>
<tr>
<td></td>
<td>(0.083)</td>
<td>(0.018)</td>
</tr>
<tr>
<td>DPA 2018: High ICO exposure × Increased penalty</td>
<td>0.535**</td>
<td>0.095**</td>
</tr>
<tr>
<td></td>
<td>(0.159)</td>
<td>(0.038)</td>
</tr>
</tbody>
</table>

| Mean | 1.15 | 0.14 |
| Industries × TTWA | Yes | No |
| Firm FE | No | Yes |
| TTWA × Year | Yes | Yes |

| Observations | 144457 | 273488 |